REQUEST FOR PROPOSALS

NKU-41-18

IT Security Audit

March 30, 2018

Proposal NO: NKU-41-18
Issue Date: March 30, 2018
Title: IT Security Audit
Purchasing Officer: Blaine Gilmore
Phone: 859.572.6449

RETURN ORIGINAL COPY OF PROPOSAL TO:

Northern Kentucky University
Procurement Services
1 Nunn Drive
617 Lucas Administrative Center
Highland Heights, KY 41099

IMPORTANT: BIDS MUST BE RECEIVED BY: 05/04/2018 BEFORE 2:00 P.M. HIGHLAND HEIGHTS, KY time.

NOTICE OF REQUIREMENTS

1. The University's General Terms and Conditions and Instructions to Bidders, viewable at http://procurement.nku.edu/policies/terms-and-conditions.html, apply to this Request for Proposal.
2. Contracts resulting from this RFP must be governed by and in accordance with the laws of the Commonwealth of Kentucky.
3. Any agreement or collusion among Offerors or prospective Offerors, which restrains, tends to restrain, or is reasonably calculated to restrain competition by agreement to bid at a fixed price or to refrain from offering, or otherwise, is prohibited.
4. Any person who violates any provisions of KRS 45A.325 shall be guilty of a felony and shall be punished by a fine of not less than five thousand dollars nor more than ten thousand dollars, or be imprisoned not less than one year nor more than five years, or both such fine and imprisonment. Any firm, corporation, or association who violates any of the provisions of KRS 45A.325 shall, upon conviction, may be fined not less than ten thousand dollars or more than twenty thousand dollars.

AUTHENTICATION OF BID AND STATEMENT OF NON-COLLUSION AND NON-CONFLICT OF INTEREST

I hereby swear (or affirm) under the penalty for false swearing as provided by KRS 523.040:

1. That I am the offeror (if the offeror is an individual), a partner, (if the offeror is a partnership), or an officer or employee of the bidding corporation having authority to sign on its behalf (if the offeror is a corporation);
2. That the attached proposal has been arrived at by the offeror independently and has been submitted without collusion with, and without any agreement, understanding or planned common course of action with, any other Contractor of materials, supplies, equipment or services described in the Request for Proposal, designed to limit independent bidding or competition;
3. That the contents of the proposal have not been communicated by the offeror or its employees or agents to any person not an employee or agent of the offeror or its surety on any bond furnished with the proposal and will not be communicated to any such person prior to the official closing of the RFP:
4. That the offeror is legally entitled to enter into contracts with the Northern Kentucky University and is not in violation of any prohibited conflict of interest, including those prohibited by the provisions of KRS 45A.330 to .340, 164.390, and
5. That the Offeror, and its affiliates, are duly registered with the Kentucky Department of Revenue to collect and remit the sale and use tax imposed by Chapter 139 to the extent required by Kentucky law and will remain registered for the duration of any contract award
6. That I have fully informed myself regarding the accuracy of the statement made above.

SWORN STATEMENT OF COMPLIANCE WITH FINANACE LAWS

In accordance with KRS45A.110 (2), the undersigned hereby swears under penalty of perjury that he/she has not knowingly violated any provision of the campaign finance laws of the Commonwealth of Kentucky and that the award of a contract to a bidder will not violate any provision of the campaign finance laws of the Commonwealth of Kentucky.

CONTRACTOR REPORT OF PRIOR VIOLATIONS OF KRS CHAPTERS 136, 139, 141, 337, 338, 341 & 342

The Contractor by signing and submitting a proposal agrees as required by 45A.485 to submit final determinations of any violations of the provisions of KRS Chapters 136, 139, 141, 337, 338, 341 and 342 that have occurred in the previous five (5) years prior to the award of a contract and agrees to remain in continuous compliance with the provisions of the statutes during the duration of any contract that may be established. Final determinations of violations of these statutes must be provided to the University by the successful Contractor prior to the award of a contract.

CERTIFICATION OF NON-SEGREGATED FACILITIES

The Contractor, by submitting a proposal, certifies that he/she is in compliance with the Code of Federal Regulations, No. 41 CFR 60-1.8(b) that prohibits the maintaining of segregated facilities.

RECIPROCAL PREFERENCE

(1) Prior to a contract being awarded to the lowest responsible and responsive bidder on a contract by a public agency, a resident bidder of the Commonwealth shall be given a preference against a nonresident bidder registered in any state that gives or requires a preference to bidders from that state. The preference shall be equal to the preference given or required by the state of the nonresident bidder.
(2) A resident bidder is an individual, partnership, association, corporation, or other business entity that, on the date the contract is first advertised or announced as available for bidding:
(a) Is authorized to transact business in the Commonwealth; and
(b) Has for one (1) year prior to and through the date of the advertisement, filed Kentucky corporate income taxes, made payments to the Kentucky unemployment insurance fund established in KRS 341.490, and maintained a Kentucky workers' compensation policy in effect.
(3) A nonresident bidder is an individual, partnership, association, corporation, or other business entity that does not meet the requirements of subsection (2) of this section.
(4) If a procurement determination results in a tie between a resident bidder and a nonresident bidder, preference shall be given to the resident bidder.
(5) This section shall apply to all contracts funded or controlled in whole or in part by a public agency.
(6) The Finance and Administration Cabinet shall maintain a list of states that give to or require a preference for their own resident bidders, including details of the preference given to such bidders, to be used by public agencies in determining resident bidder preferences. The cabinet shall also promulgate administrative regulations in accordance with KRS Chapter 13A establishing the procedure by which the preferences required by this section shall be given.
(7) The preference for resident bidders shall not be given if the preference conflicts with federal law.
(8) Any public agency soliciting or advertising for bids for contracts shall make KRS 45A.490 to 45A.494 part of the solicitation or advertisement for bids

DEFINITIONS

As used in KRS 45A.490 to 45A.494: (1) "Contract" means any agreement of a public agency, including grants and orders, for the purchase or disposal of supplies, services, construction, or any other item; and

(2) "Public agency" has the same meaning as in KRS 61.805.

SIGNATURE REQUIRED: This proposal cannot be considered valid unless signed and dated by an authorized agent of the offeror. Type or print the signatory's name, title, address, phone number and fax number in the spaces provided. Offers signed by an agent are to be accompanied by evidence of his/her authority unless such evidence has been previously furnished to the issuing office. Your signature is acceptance to the Terms and conditions above.

DELIVERY TIME:	**NAME OF COMPANY:**	**DUNS #**
PROPOSAL FIRM THROUGH:	**ADDRESS:**	**Phone/Fax:**
PAYMENT TERMS:	**CITY, STATE & ZIP CODE:**	**E-MAIL:**
SHIPPING TERMS: F.O.B. DESTINATION - PREPAID AND ALLOWED	**TYPED OR PRINTED NAME:**	**WEB ADDRESS:**
FEDERAL EMPLOYER ID NO.:	**SIGNATURE:**	**DATE:**

Project Name:	**IT Security Audit**
Issue Date:	**March 30, 2018**
Deadline for Questions:	**April 20, 2018 @ Noon**
Addenda Issued (if applicable)	**April 27,2018 by 2 PM**
Response Deadline (Proposals Due):	**May 4, 2018 by 2 PM**

Submittal of Proposals
The bidder shall submit, by the time and date specified via US Postal Service, courier or other delivery service, its bid response in a **sealed package** addressed to:

Blaine Gilmore
Interim Director, Procurement Services
Lucas Administrative Center, Suite 617
1 Nunn Drive
Northern Kentucky University
Highland Heights, KY 41099

NOTE: Northern Kentucky University, as an Agency of the Commonwealth of Kentucky, is subject to Kentucky's Open Records Laws (KRS 61.870-61.884). As such, a bidder's entire offer and resulting contract cannot be deemed "confidential".

Proposals submitted in response to an RFP will remain confidential throughout the evaluation process, however, after negotiations are concluded and a contract has been entered into, all proposals become a matter of public record. Bidders may mark sections of their responses as confidential if the information provided would be considered financially sensitive or trade secrets. The university will make every effort to honor such requests, but may conduct discussions with the bidders concerning the release of said information.

DO NOT contact the committee members relative to this project. Contacting the selection committee members may result in disqualification of the proposer. All requests for information, questions or comments relative to this project should be directed to:

Ryan Straus
Bid Specialist
Northern Kentucky University
Lucas Administrative Center, 617
Highland Heights, KY 41099 Email: strausr2@nku.edu
FAX: 859.572.6995

NOTE: Information relative to this project obtained from other sources, including other university administration, faculty or staff may not be accurate, will not be considered binding and could adversely affect the potential for selection of your proposal.

I. General Background for RFP

A. General Scope:

The purpose of the security assessment is to test the targeted network's ability to withstand attacks from both inside and outside the network perimeter, and an analysis of potential vulnerabilities that could result from poor or improper system configuration, both known and unknown hardware or software flaws, or operational weaknesses in process, infrastructure, reporting, logging and preventative measures. The overall objectives are to identify potential vulnerabilities within the internal network and identify weaknesses within network controls, reporting, logging, and to prevent and/or detect their exploitation by a hacker/malicious employee/contractor who may obtain access to information resources, cause system disruption or a system outage. To include traditional Pen Testing, Physical Security test, and other assessments (ex, wireless). Audit tests would need to be performed at times that are conducive to NKU academic and business schedules, such as maintenance windows.

B. Contract

This is a one-time audit services contract. The resulting contract from this RFP will expire at the completion of the project. NKU expects completion of work within 4 weeks and final presentation within 6 weeks of contract

C. Responsiveness

The objective of the selection process is to provide a uniform methodology for Northern Kentucky University to procure IT audit services. Members of the selection committee are asked to fairly evaluate all responses and to compare each team's qualifications with the project requirements. Selections will be determined through the unbiased and independent interaction of the members of the committee. Therefore, it is in your firm's best interest to be specifically responsive to the requirements of this solicitation.

Respondents shall be limited to one proposal per respondent per project. For the purposes herein, a "respondent" means the legal entity which responds to an RFP. Multiple respondent proposals per project will all be deemed as being non-responsive. By submitting qualifications, the respondent represents that it has thoroughly examined and become familiar with the work required under this RFP and that it is capable of performing quality work to achieve the university's objectives. Note: Sub-consultants can be a member of more than one team.

II. Northern Kentucky University

A. BRIEF DESCRIPTION OF THE UNIVERSITY

Founded in 1968, today NKU enrolls more than 14,000 students, with 2,000 students residing on campus. Named among "America's Top Colleges" by *Forbes* for eight consecutive years, NKU is noted for its commitment to excellence in the classroom, innovative and nationally-ranked academic programs, commitment to diversity and inclusion, and for leading the way in regional stewardship and service learning. Our 17 athletic programs recently completed the transition to NCAA Division I competition and are eligible to compete for NCAA Division I championships for the first time. For 11 consecutive semesters, our student-athletes have also posted a cumulative GPA of 3.0 or better, including 3.28 in Fall 2016.

NKU offers 76 undergraduate, 21 master's programs, two professional doctorates and a juris doctor. The university features six colleges – the College of Arts and Sciences, the Haile/US Bank College of Business, the College of Education and Human Services, the College of Health Professions, the College of Informatics, and the Salmon P. Chase College of Law. The College of Arts and Sciences is also home to our nationally-known School of the Arts, and work is underway to create an Honors College.

NKU's educational quality is also at an all-time high. With an average class size of just 24 and a

student/faculty ratio of 18:1, NKU's hallmark is small classes with up-close and personal attention to student needs. The Princeton Review has named NKU's College of Business among America's best, and Chase law graduates routinely outperform their peers on the Kentucky and Ohio Bar Exams. The average ACT score for incoming NKU freshmen is 23.9 – up significantly since the adoption of new admission standards and higher than the Kentucky and national averages. We are also committed to success for all students, reflected in the 6 percent growth in our first-to-second-year retention rate since 2010, far exceeding the national average.

In 2018, NKU will open a new academic facility, the Health Innovation Center, which will be home to the College of Health Professions and to transdisciplinary programs that will position us to address the most important population health challenges confronting our region and the nation, including the crisis of opioid addiction.

NKU's information systems infrastructure is composed of 2 Network cores, 11 buildings with a primary routers, 350 switches, and 800 wireless access points. Wireless has both public and organization access. Servers include 200 Windows Servers, 50 Linux, and others. 5,000 managed endpoints. 8,000 BYOD undocumented devices a day on the network. IT has 80 employees.

As we prepare to celebrate our 50th anniversary, we are on the rise.

III. Specifications / Scope of Work

Objectives of the Security and Network Audit

1. If PII is discovered during the audit then NKU must be notified immediately to resolve.
2. Identification of security vulnerabilities that may affect NKU Business Services.
    a. Does not include student owned devices.
3. Requirements and analysis performed to increase overall security.
4. Perform penetration testing that assists with regulatory compliance standards and the NIST 800-53 controls.
5. Risk Assessment to Identify and prioritization of risks to the University, with suggestions for risk mitigation and security improvements.

NKU personnel will be available to answer questions about the network and server architecture, as well as current security procedures and controls. This will allow the auditor to attempt penetration with full knowledge. NKU will need to be notified if credentials are needed for specific test. Specific Rules of Engagement and the Audit Plan will exist to ensure desired coverage is accomplished. NKU and the selected vendor will provide project management. The project managers will monitor the engagement to ensure that the Rules of Engagement are followed and the objectives in the detailed audit plan developed in the audit are met.

Perform the audit and testing in such a way that NKU business and services will not affected or disrupted in any way. If a disruption is possible then an agreed upon time and/or exception will be needed.

Section I: Internal Assessment

Objectives: The purpose of the internal assessment is to test the targeted network's ability to withstand attack inside the network perimeter, and an analysis of potential vulnerabilities that could result from poor or improper system configuration, both known and unknown hardware or software flaws, or operational weaknesses in process, infrastructure, reporting, logging and preventative measures. The overall objectives are to identify potential vulnerabilities within the internal network and identify weaknesses within network controls, reporting, logging, and to prevent and/or detect their exploitation by a hacker/malicious employee/contractor who may obtain access to information resources, cause system disruption or a system outage. At a minimum, the audit should include:

- Network Discovery: Ascertain the internal network topology or footprint that provides a map of the critical access paths/points and devices including their Internet protocol (IP) address ranges. Identify architecture/topology faults with in the network routers/switches..
- Vulnerability Analysis: Once project management agrees on the critical points/devices within the network, attack those devices given the various types of known vulnerabilities within the system and operating software running on the devices.
- Exploitation: Determine the level of attack that NKU desires and approves, assuring no disruption of systems or services during the tests. Time of attack or exceptions may be needed to reduce Business impact. Determine the level of attack based on the level of access obtained on the open ports and the target hosts identified by the discovery and analysis stages, or on the basis of information provided by NKU.
    - From an on-site location, attempt to penetrate the internal network.
    - Members of the penetration team connect to the NKU's internal network and attempt to compromise the servers, workstations, and routers.
    - Using compromised accounts, the penetration team uses a series of exploits to attempt to gain root or administrative access to servers, network equipment and other machines in the network. The penetration team identifies the damage that can be done (places files, harvests files, etc.) once root is captured on any of these machines.

  - Once the penetration team captures root on one machine, attempt attacks on other machines in the network from compromised computer. Document all machines they are able to access, the type of capabilities they gained, and harvest some files to prove access.
  - Using the root capabilities on a machine within the network, the penetration team attacks the firewall and Internet connections from the inside.
  - Notify NKU if access level is achieved
  - Record all vulnerabilities noted and provide to NKU for immediate follow-up at the conclusion of the penetration test/vulnerability analysis.
  - Any entry points discovered by the tests are documented. The entry points are exploited in an attempt to penetrate the network
- The tester review and assess the Intrusion detection response (including logs).
- The tester will perform a review of network logs and available reporting, and report weaknesses as well as improvement opportunities for logging, reporting tools and detection techniques.

Section II: Physical Security

Objectives: Physical Security factors of the data center and data closets should be evaluated for physical safety and security. Factors to be considered include, but are not limited to:

- Review of the equipment safety and protection from physical elements such as dust, water, temperature controls, and other physical factors.
- Review location of critical equipment - secure, locked, and isolated from access and limited to authorized staff.
- Review of cameras and their monitoring.
- Review of power and emergency (fire, heat, water) protection.
- Report of physical vulnerabilities - prioritized and documented, along with suggestions for improvements.

Section III: Wireless Assessment

Objectives: The purpose of the wireless assessment is to test its ability to withstand attack. The overall objective is to identify potential vulnerabilities within the wireless network and weaknesses in controls in place to prevent and/or detect their exploitation by a hacker/malicious employee/contractor who may obtain access to information resources, cause system disruption or a system outage. At a minimum, the audit objectives must include:

- Network Discovery: Ascertain the internal network topology or footprint that provides a map of the critical access paths/points and devices including their Internet protocol (IP) address ranges. Also review of trust boundaries for the different networks/SSID.
- Vulnerability Analysis: Once critical points/devices are identified within the network, attack those devices given the various types of known vulnerabilities within the system and operating software running on the devices.
- Exploitation: Determine the level of attack that NKU desires and approves, assuring no disruption of systems or services. Determine the level of attack based on the level of access obtained on the open ports and the target hosts identified by the discovery and analysis stages, or on the basis of information provided by NKU.
  - From an on-site location, attempt to penetrate the internal network.
  - Members of the penetration team connect to the NKU's internal network and attempt to compromise the servers, workstations, and routers.
  - Using compromised accounts, the penetration team uses a series of exploits to attempt to gain root or administrative access to servers, network equipment and other machines in the network. The penetration team identifies the damage that can be done (places files, harvests files, etc.) once root is captured on any of these machines.
  - Once the penetration team captures root on one machine, they should attempt attacks on other machines in the network from compromised computer. Document all machines they

are able to access, the type of capabilities they gained, and harvest some files to prove access.
    - Using the root capabilities on a machine within the network, the penetration team attacks the firewall and Internet connections from the inside.
    - Notify NKU if access level is achieved
    - Record all vulnerabilities noted and provide to NKU for immediate follow-up at the conclusion of the penetration test/vulnerability analysis.
    - Any entry points discovered by the tests are documented. The entry points are exploited in an attempt to penetrate the network
- Intrusion detection response (including logs) reviewed and assessed.
- Perform a review of all network logs and available reporting, and report weaknesses as well as improvement opportunities for logging and reporting tools and detection techniques.
    - Recommendations should be vendor independent and should support the current NKU architecture
    - Recommendations should be a minimum of 3 tool(s) or reporting systems.
    - Recommendations could include both Commercial and Open Source products.

Section IV: Internet Assessment & Web Assessment

Objectives. The purpose of the Internet assessment is to test the targeted network for vulnerability analysis and exploitation via the Internet. The test methodology will allow for a systematic checking for known vulnerabilities and pursuit of potential security risks.

At a minimum, the audit objectives should include vulnerability analysis and exploitation. Methodology to include but not inclusively defined:

- From a remote (non-NKU) site, attempt penetration from the Internet.
- A determined Internet attack from multiple locations over an extended period is launched.
- Any weaknesses identified are exploited using non-intrusive techniques to harvest files, insert files into the network (simple text files) and hop between servers to compile a network diagram and document additional exploits.
- The firewall is to be tested. In addition to non-invasive techniques, techniques that are designed to momentarily disable the firewall are used if it was improperly configured.
- The VPN is to be tested for security and connectivity/remote access.
- NKU's wireless local area network will be tested for secure configuration including but not limited to rogue access points, encryption strength, access rights and coverage leakage.
- Using common hacking methods (such as cross site scripting, SQL injection) try to gain access to private data or deface 5 different service websites ('Email Login, Password Change Page, myNKU and www). Also, identify potential weaknesses in web code design on these pages.

Section V: Gramm Leach Bliley Act Assessment

Objectives. The purpose of the GLB assessment is to look for gaps and recommendations for NKU compliance. This compliance requirement is new to NKU.

At a minimum, the audit objectives should include: compliance items currently in place, compliance items that are needed, and documentation and/or mapping to assure future compliance of GLB with flexibility for future compliance regulations.

- Employee or employees to coordinate the information security program.
- Identify reasonable, foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, destruction, or other

compromise of such information and assess the sufficiency of any safeguards in place to control these risks

- At a minimum, such a risk assessment should include consideration of risks in each of the following operational areas:
    - Employee training and management
    - Information systems, including network and software design as well as information processing
    - Storage, transmission, and disposal and
    - Detecting, preventing, and responding to attacks, intrusions or other system failures
- Design and implement information safeguards to control the risks identified through risk assessment and regularly test or monitor the effectiveness of the safeguards key controls, systems and procedures
- Oversee service providers by taking steps to select and retain providers that are capable of maintaining appropriate safeguards for customer information
- Contractually require service providers to implement and maintain such safeguards

Section VI: Risk Assessment

Objectives. The purpose of the Risk Assessment is to identify gaps in NKU Risk Assessment process. Recommendations for improvements and/or tools to assist in the business process

At a minimum, the objectives should include: Methodology to include but not inclusively defined:

- Business area reviews.
- Risk Assessment reviews.
- Documentation of reviews.
- Other items to be identified as needed.

Deliverables

The purpose of the audit is to report security improvements, to identify the weaknesses, develop NKU-specific recommendations to address weaknesses, and communicate results to NKU. The final deliverable will be defined prior to engagement, to include the following:

- All observations will be thoroughly discussed with appropriate and related IT management before finalization report
- Include an executive summary and overview
- A presentation to technical and security staff
- Schedule and prioritization of actions based on risk to the university
- Summary of reviewed policies and procedures with recommendation for changes, additions, or deletions
- Compliance standard recommendations for periodic penetration tests
- Regulations that may be in scope for the University. Examples: HIPAA-HITECH, GLBA, FERPA, State Breach Notification Laws, GDPR.
- Additional technical detail will be available as support information to answer questions
- Identification of tests, tools used and results of tests
- Specific gaps, deficiencies, vulnerabilities observed
- In addition to the assessment and findings, make specific recommendations as to how findings can be remedied
- List of vulnerabilities penetrated
- Detailed analysis of strengths and weaknesses sufficient to build a mitigation plan.
- Recommendations for a continuous audit approach
- Details per the assessment sections as follows:

    Section I: Internal Assessment Specifics
    - Review of architecture/topology of routers and switches and their configurations.

- Servers
  - Active Directory and the NKU domain.
  - E-mail
  - Patch Management
  - Compliance standards
  - Etc.
- Recommendations for improvements and course of action
- Recommendations for logging, reporting, and Intrusion Detection system

Section II: Physical Assessment Specifics

- Location reviews, device hardening improvements
- Employee Access reviews
- Environmental (fire, water, dust, physical) reviews
- Recommendations for improvements and course of action
- Access controls
- Camera reviews

Section III: Wireless Assessment Specifics

- Review of wireless current and future wireless goals, objectives
- Growth path to ensure security and growth as needed for current and future mobility across campus
- Recommendations for improvements and course of action

Section IV: Internet Assessment Specifics

- Review and analysis of VPN Security
  - Site to Site Tunnels
  - Remote Access
- Review of firewall security
  - Design and Architecture
  - Identification of gaps in access list
- Vulnerability of all Internet accessible hosts, websites, and application coding.
- Recommendations to reduce web vulnerabilities and improve development coding methods.
- Review of protocols, SSLv3, TLS 1.0, and TLS 1.1.

Section V: Gramm Leach Bliley Act

- Compliance requirements currently in place.
- Requirements needed.
- Documentation process for compliance.

Section VI: Risk Assessment

- Risk Assessment Report
- Business Area Review
- Recommendations to prioritize risk.

A presentation to an executive group that would entail a summary of results with actual examples to illustrate points may be required. The presentation will include descriptions of methodologies be kept very brief with the focus on the overall level of risk within the network and the types of actions that will be necessary to reduce risk. Descriptions of the types of vulnerabilities may be used, but where possible, specific system identification will be avoided to prevent the focus from being diverted from larger problems to more specific and familiar system-specific problems. The presentations, as well as the final report itself, must be written to identify the weaknesses

and lay out a roadmap to mitigate unnecessary risk in the network, and identify improvement opportunities in process, procedures, infrastructure, and logging tools.

NKU Project Special Conditions

- Confidentiality agreement must signed by awarded contractor before work may begin
- Expect work completion within 4 weeks and final presentation within 6 weeks of contract.
- Sections may be awarded separately or to an individual vendor.
- Scope of sections may be tailored to make best use of budgeted amount.

Pricing

Should be presented for the following 6 sections including, hours of labor, administrative cost for reporting, presentation, material, etc.

I. Internal Assessment	
Estimated Hours	
Administrative Cost	$
Other	$
Total Cost	$

II. Physical Security	
Estimated Hours	
Administrative Cost	$
Other	$
Total Cost	$

III. Wireless Assessment	
Estimated Hours	
Administrative Cost	$
Other	$
Total Cost	$

IV. Internet & Web Assessment	
Estimated Hours	
Administrative Cost	$
Other	$
Total Cost	$

V. Gramm Leach Bliley Act Compliance	
Estimated Hours	
Administrative Cost	$
Other	$
Total Cost	$

VI. Risk Assessment	
Estimated Hours	
Administrative Cost	$
Other	$
Total Cost	$

Total Assessment	
Estimated Hours	
Administrative Cost	$
Other	$
Total Cost	$

Pricing with discounts noted for successfully obtaining 3 sections

IV. Proposal

A. Preparation and Submission of Proposal

The proposal shall be prepared on 8 ½" x 11" paper, with all text clear of binding. Text type size shall be a minimum of 10 point font. The proposals must be indexed, tabbed and all pages sequentially numbered throughout or by section. Binders and covers will be at the respondent's discretion, however, elaborate graphics and expensive paper and binding are not necessary, nor encouraged. All text and exhibits should be concise and entirely relevant to the RFP requirements.

The RFP Response should be organized as follows:

Tab	Content
1	Signed Authentication of Bid and Statement of Non-Collusion and Non-Conflict of Interest (Pages 2/3)
2	Cover Letter
3	Background, Experience, and References
4	Pricing Structure (Page 12 of the RFP Document)

NOTE: Submittals that do NOT contain the above items will be deemed a non-responsive proposal and disqualified from the selection for this project.

The respondent shall submit, via US Postal Service, courier or other delivery service, six bound copies, one unbound original, and one digital (USB, CD, SD Card) copy of its proposal in a sealed package by **May 4, 2018 @ 2pm**. Failure to provide the required number of copies and an unbound original will result in the submittal being considered non-responsive and disqualified from the selection process. Submittals shall be addressed to:

Blaine Gilmore
Interim Director, Procurement Services
Lucas Administrative Center, Suite 617
1 Nunn Drive
Northern Kentucky University
Highland Heights, KY 41099

Bearing respondent's name and address, and clearly marked as follows:
RFP NKU-41-18
IT Security Audit

B. Proposal Requirements and Specifications

1. Signed Authentication of Bid and Statement of Non-Collusion and Non-Conflict of Interest

Please review and sign page 2/3 of this document. Place the signed original in the original copy of your proposal.

2. Cover Letter

The cover letter shall serve as an introduction to the Respondent's qualifications and capabilities. The letter of no more than 2 pages shall be addressed to Blaine Gilmore, Interim Director of Procurement Services, and must, at a minimum, contain the following:

a. Identification of vendor.
b. A brief statement of experience from the contractor (years in business etc).
c. Contact information including email address
d. Acknowledgement of receipt of RFP addenda, if any; and,
e. Signature of person authorized to bind the offering firm to the terms of the Proposal.

3. Pricing Structure

Proposer shall provide pricing information for each individual assessment as well as a total price. Please see page 12.

4. Background, Experience, and References

Please include short bios of key personnel as well as qualifications / credentials of employees performing the test

Identify other clients in which you have provided IT auditing services for in the past. Ideally, these clients should have a similar background as Northern Kentucky University; however it is not required.

For each client, provide a name, email address, and telephone number for a contact person who is familiar with the contractor's services. The contact person should be familiar with the key personnel.

C. Evaluation Criteria

The detailed specifications and special terms and conditions describe those items considered essential for a comprehensive agreement, while allowing proposers sufficient latitude to make comprehensive and creative proposals to the University.

Award will be made to the proposer whose proposal, in the sole opinion of the University, represents the best overall interests of the University, considering but not limited to the following:

	%
Pricing Structure	35%
Ability to perform work based on background / experience	40%
Reference check	25%
Total	**100%**

V. Special Conditions

A. Addenda/Clarifications

Any university changes to this RFP will be made by written addendum. Verbal modifications will not be binding.

B. Confidentiality

In accordance with KRS 45A.085 Competitive Negotiation, all proposals received or information derived therefrom remain confidential until a contract is awarded or all proposals are rejected.

C. Proposal Evaluation Process

All proposals received will be reviewed by the University Procurement Services office for completeness of items requested in this RFP. All complete proposal responses will be afforded equal consideration by the members of the Selection Committee as created by KRS 45A.810 and whose members are identified above. All complete proposals will be evaluated using a numerical rating system designed to afford each Selection Committee member a reasonable, individual, objective standard to equate the qualifications of the Respondents.

D. Pre-Contractual Expenses

Pre-contractual expenses are defined as expenses incurred by the respondent in:

1. preparing its proposal in response to this RFP;
2. submitting its qualifications to the university;
3. negotiating with the university any matter related to this submittal; or,
4. any other expenses incurred by a respondent prior to the date of award of a contract to the selected respondent.

The university shall not, in any event, be liable for any pre-contractual expenses incurred by the respondents in the preparation of their submittals.

E. Contract Award

Issuance of this RFP, receipt of proposals, and completion of the selection process does not commit the university to award a contract. The university reserves the right to postpone opening for its own convenience, to accept or reject any or all proposals received in response to their RFP; to negotiate with other than the selected respondent should negotiations with the selected firm be unsuccessful or terminated; to negotiate with more than one respondent simultaneously; to cancel all or part of the RFP; and to waive technicalities.

F. Electronic Responses

Electronic responses are not permitted.

G. Foreign Corporations

1. Foreign Corporations are defined as corporations that are organized under laws other than the laws of the Commonwealth of Kentucky. Foreign Corporations doing business within the Commonwealth of Kentucky are required to be registered with the Secretary of State, New Capitol Building, Frankfort, Kentucky and must be in good standing.

2. The Foreign Corporate Proposer, if not registered with the Secretary of State at the time of the Bid submittal, shall be required to become registered and be declared in good standing prior to the issuance or receipt of a contract.

3. Domestic Corporations. Domestic corporations are required to be in good standing with the requirements and provisions of the Office of the Secretary of State.

H. Occupational License

Northern Kentucky University was annexed by the City of Highland Heights in 2008. All contractors performing work for NKU must possess a Campbell County Occupational License and a City of Highland Heights Occupational License (administered by Campbell County) and must also pay applicable payroll taxes. For further information call 859.292.3884 or log onto: http://www.campbellcountyky.org/home/services/occupational-license.htm.

I. Insurance

Vendor must provide NKU with an insurance certificate listing NKU as a certificate holder and additionally insured.

Northern Kentucky University
617 Lucas Administrative Center
1 Nunn Drive
Highland Heights, KY 41099

The Contractor shall furnish the University the Certificates of Insurance and guarantee the maintenance of such coverage during the term of the contract. The Contractor shall provide an original policy endorsement of its CGL insurance naming Northern Kentucky University and the directors, officers, trustees, and employees of the University as additional insured on a primary and non-contributory basis as their interest appears. Additionally, the Contractor shall provide an original policy endorsement for Waiver of subrogation in favor of the Northern Kentucky University its directors, officers, trustees, and employees as additional insured.

Our basic insurance requirements are:
Worker's Compensation and Employers' Liability Insurance: the Contractor shall acquire and maintain Workers' Compensation insurance with Kentucky's statutory limits and Employers' Liability insurance with at least $100,000 limits of liability.

Comprehensive General Liability (CGL) Insurance the limits of liability shall not be less than $500,000 each occurrence for bodily injury and $250,000 property damage.

Comprehensive Automobile Liability Insurance: To cover all owned, hired, leased or non-owned vehicles used on the Project. Coverage shall be for all vehicles including off the road tractors, cranes and rigging equipment and include pollution liability from vehicle upset or overturn. Policy limits shall not be less than $500,000 for bodily injury and $100,000 for property damage.

Excess liability insurance in an umbrella form for excess coverages shall have a minimum of $1,000,000 combined single limits for bodily injury and property damage for each.

If accessing NKU Student, Employee, or other personal records, vendor needs Security and Privacy Liability Insurance with limits no less than $1,000,000.

If accessing NKU Student, Employee, or other personal records, vendor needs Evidence Breach Response Services coverage with limits no less than $5,000,000.

J. Personal Services Contract

This RFP is for consulting, auditing or other personal services. Kentucky law requires a Personal Services Contract to be signed by the vendor and filed with the Legislative Research Commission in Frankfort prior to any work beginning. KRS 45A.690 defines a Personal Service Contract as "an agreement whereby an individual, firm, partnership, or corporation is to perform certain services requiring professional skill or professional judgment for a specified period of time at a price agreed upon."

After Determination but prior to award, a Personal Services Contract will be sent to the winning offeror for signature. Please be sure to sign and return the **original** contract promptly to Northern Kentucky University. A Notice of Award will not be issued until the signed Personal Services Contract has been received by Procurement Services and filed with the Legislative Research Commission in Frankfort, KY.

REGARDING PERSONAL SERVICE CONTRACT INVOICING

House Bill 387 has now amended Kentucky Revised Statute 45A.695(10)(A) with the following language, "No payment shall be made on any personal service contract unless the individual, firm, partnership, or corporation awarded the personal service contract submits its invoice for payment on a form established by the committee". The Personal Service Contract Invoice Form shall be used for this purpose and for you convenience we have added fields so that it can be filled in online and printed. This form can be located on NKU's Procurement Services website at: http://procurement.nku.edu/departmental_forms/PSC_INVOICE_FORM.pdf